Genuinely Secure Systems

Bill Worley, CTO

Secure64 Software Corp.

April 2007

SECURE64

SOFTWARE CORPORATION

Introduction

- Network-based BAD guys are winning
  - Vulnerabilities are UP, CERT 12 July 2006
  - Security products are vulnerable, Secunia 12 July 2006
  - IBM: More Vulnerabilities in '07, eWeek 30 January 2007
  - DNS: Definitely Not Safe, CSOonline 2 February 2007
  - Verisign: Cyberattacks up by 50% by 2010, InformationWeek 8 February 2007
  - DNS attack traffic up 150 fold since 2000, InfoWorld 16 February 2007
  - Dangerous Flaw in Microsoft DNS Server, NetworkWorld 13 April 2007
- Horizon: Emerging Security Technologies
  - Vista© operating system
  - S/W: Virtualization
  - H/W: VT + TPM + LT + VT-d
  - Powerful & Necessary, but Insufficient
- GOOD GUY Assets: Dual-core Itanium® 2 processors
  - Unique (but not widely utilized) security capabilities
  - Capabilities crucial for Genuinely Secure System

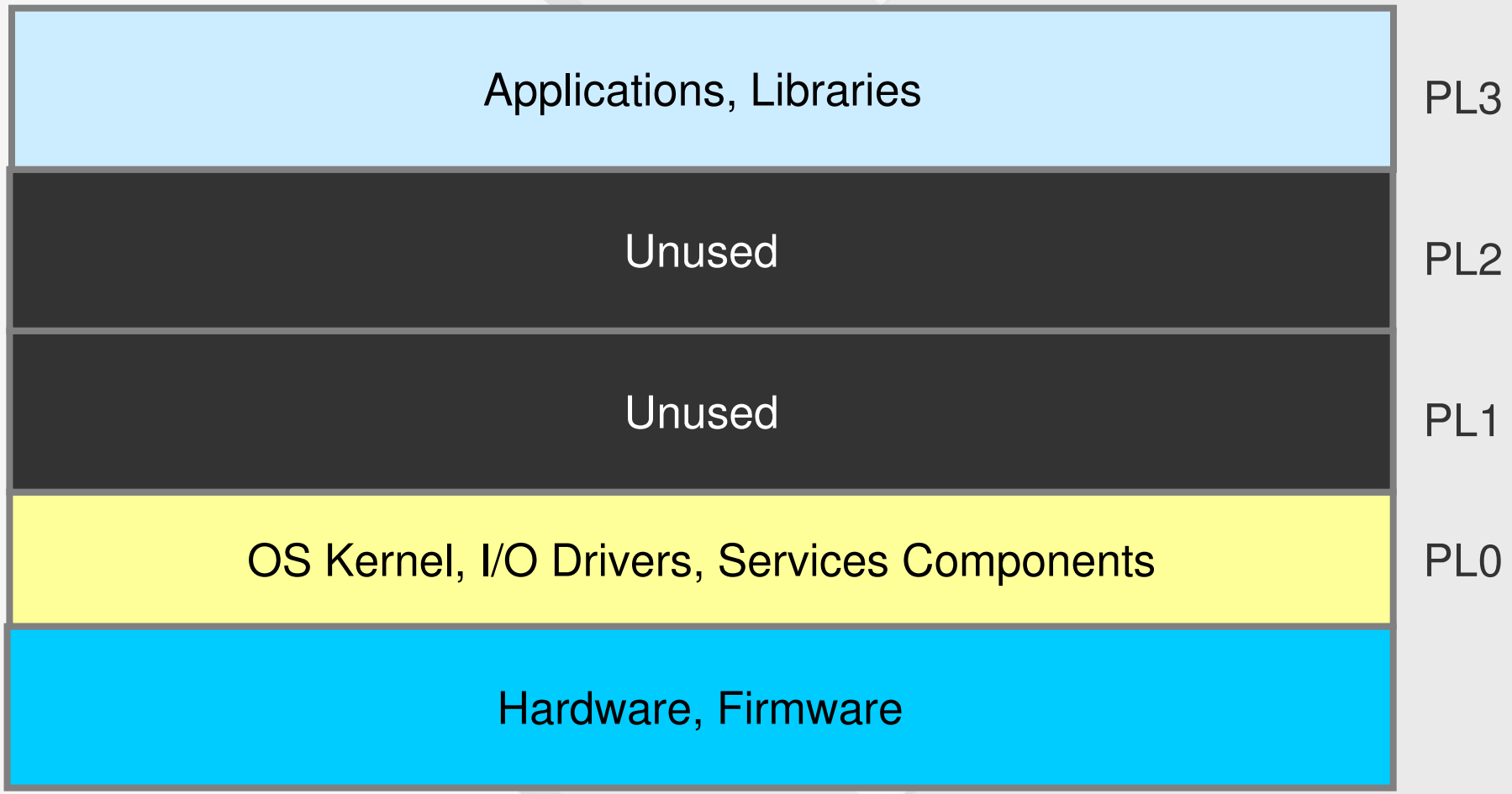
SECURE64

Topics

- Root causes of system S/W vulnerabilities
- Definition of Genuinely Secure System
  - How addresses root causes of vulnerabilities
- Emerging H/W & S/W technologies
  - Why: Not sufficient for Genuinely Secure Systems
- Unique Itanium® 2 architecture capabilities
  - Today, Tomorrow
- Architecture for Genuinely Secure System
  - Synthesis of emerging trends, unique architecture
- Conclusions and Summary

SECURE64

Today's Software Structure



SECURE64

Root Causes of S/W Vulnerabilities

- Imperfect Code
- Excessive Code & Complexity at Highest Priv Level (PL0)
- Static, Coarse-Grained Hardware Isolation & Protection
- Vulnerable Code and Data (Memory and Disk)
- Landing Sites for Code Injection
  - Rootkits, Viruses, Other Malware
- Unprotected I/O Architecture
  - Orthogonal to H/W Memory Protections
- OS's, Network Stacks
  - Not Designed to Withstand Malice
  - Not Designed to generate, retain, use, safeguard secrets
  - Not Designed to Guarantee Strong Security Properties.

SECURE64

Genuinely Secure System

- Definition: Systems with specific Technical Properties
  - Different from General-Purpose O/S Properties
  - Required in System S/W Foundation Layer(s)
    - For Vanilla/Virtualized, Proc-Ctl/Network/Server Systems
- P1: Fully Authenticated Boot Process
  - Root Trust
  - Firmware and Software
- P2: Only Minimum Mechanisms at PL0
  - Comprehensible, auditable by single persons, < 10KLOC
  - Published for expert, peer review
  - No I/O Drivers at PL0
- P3: Trusted Calls to PL0 Mechanisms
  - Only authorized call paths to alter H/W state
- P4: Eliminate ALL Code Injection
  - Disk and Memory

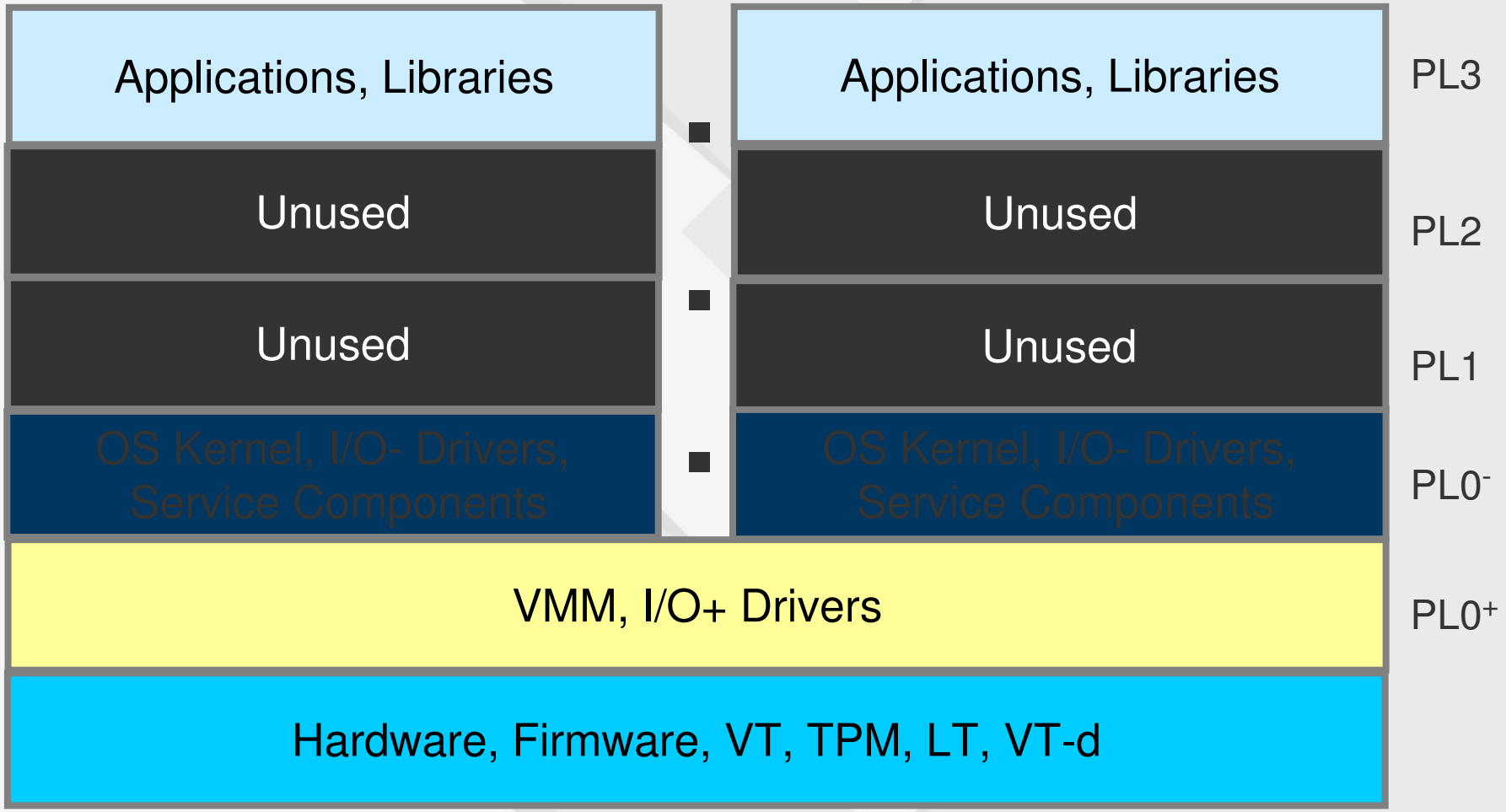
SECURE64

Genuinely Secure System (Cont'd)

- P5: Fine-Grained, Static & Dynamic H/W Isolation
  - Compartmentalized Memory
  - Dynamic Compartment Control
- P6: H/W Isolation of Critical Information
  - Stacks, Resource Allocation Info
  - On-Demand Compartments for ALL Secrets
  - Compartments for I/O Driver Isolation
  - I/O Drivers use Virtual Addresses, PL0 Mechanisms
- P7: Encrypt and Authenticate Critical Information on Disk
- P8: Self-Protecting Network Stack
- P9: Granular Authorization Categories
  - Role based, Multi-Factor Authentication

SECURE64

Emerging H/W, S/W Technologies



SECURE64

Observations

- Important security advances are happening
  - More attention to system security
  - H/W generation, retention of root secrets
  - H/W generation of random numbers
  - Enable encrypted software distribution
  - Integrated I/O & memory H/W protections
  - Strong benefits for operating system implementations
- But, by themselves, the emerging technologies:
  - Don't address all root system S/W weaknesses
  - Missing important security capabilities
  - Generate new problems and vulnerabilities
  - Cannot produce genuinely secure system

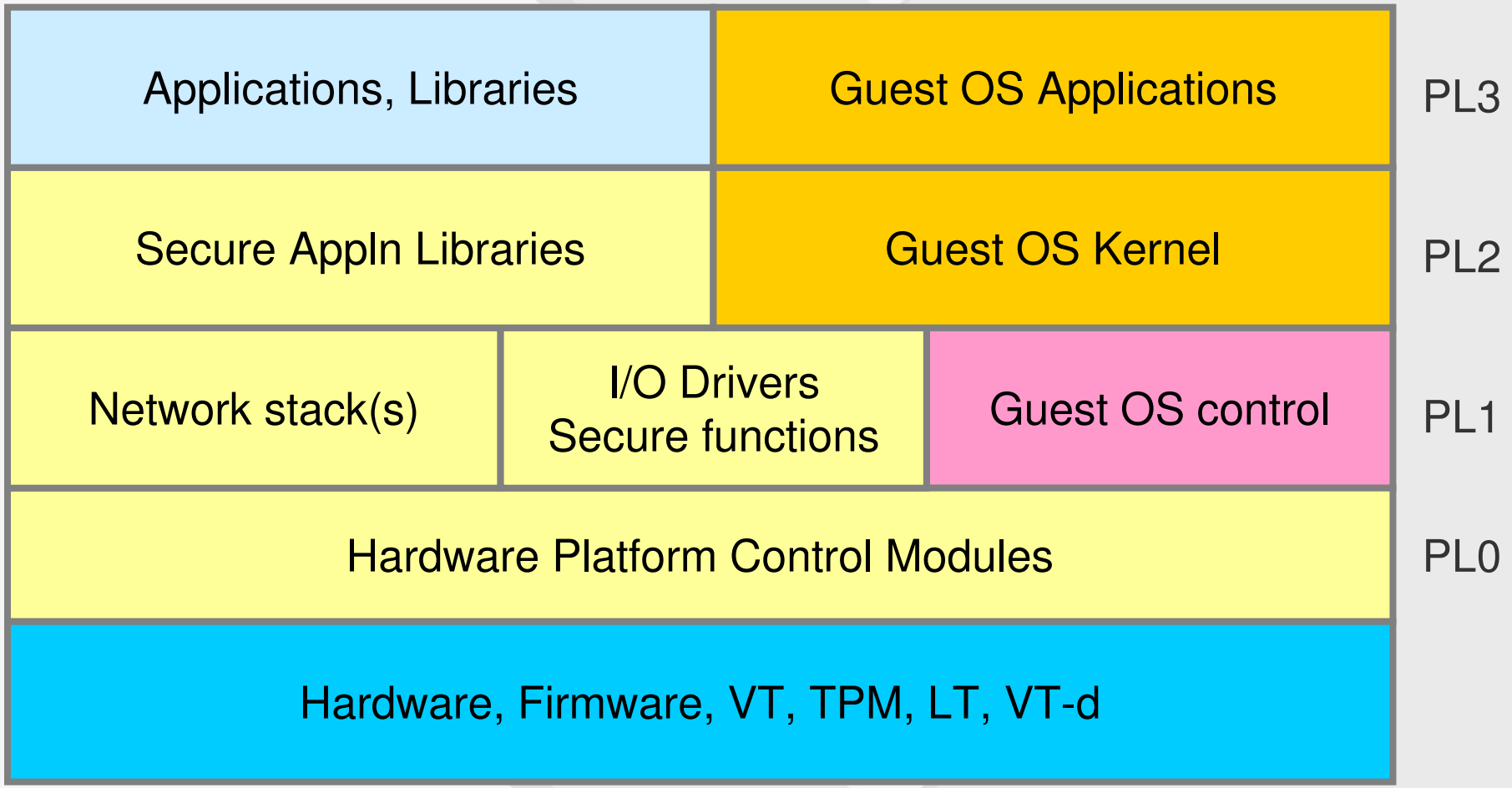
SECURE64

Itanium® 2 Architecture Capabilities

- Four static hardware privilege levels, PL0-PL3
- Virtual page compartments (Unique)
  - 12 page sizes, from 4K bytes to 4G bytes
  - Page access rights: R/W/X as function of H/W privilege level
  - Page protection keys: 16.7M IDs; R/W/X disable bits
- Interruptions retain mappings, protections (Unique)
- Register Save Engine (Unique)
  - save/restore registers in protected pages
- Enhanced H/W authentication of firmware (Unique)
- Emerging: VT-i + TPM + LT + VT-d Extensions

SECURE64

Architecture for Genuine Security



SECURE64

Secure64 DNS

Secure64 DNS

DoS-resistant DNS for the Always-on Business

DNS has emerged as one of the weakest links in IT infrastructures. Denial-of-service attacks and remotely exploitable security vulnerabilities threaten both the availability and integrity of existing DNS solutions. *And if DNS is down, the web is down, email is down, and your business is down.*

Availability under attack

Secure64™ DNS withstands denial-of-service attacks up to the saturation point of a Gigabit line while still responding to legitimate queries, unlike other DNS applications that can fail during network attacks.

Genuinely secure not hardened

Secure64 DNS is the first application to run on SourceT®, a micro OS designed from the ground up for security and performance. Unlike hardened operating systems, SourceT is genuinely secure, designed to fully utilize the hardware to make the system and its applications immune to compromise from rootkits and malware and resistant to network attacks.

Highest performing DNS

In addition, SourceT's high speed network I/O stack dramatically improves DNS query performance. This allows Secure64 DNS to achieve over 100,000 queries per second, the highest performance of any authoritative DNS solution.

Key Benefits

- Maintains performance during denial-of-service attacks
- Removes risk of security breach from malicious code
- Eliminates the need for OS hardening
- Allows consolidation of DNS servers

Key Features

- Highest performance of any authoritative DNS solution
- Built-in denial-of-service detection and mitigation
- Immune to injection of rootkits and malware
- Compatible with the latest versions of BIND and Microsoft DNS

Availability Under Attack

SECURE64

- Genuinely secure, not hardened
- HP 2660 2RU server
  - Single dual core Itanium® chip
- Withstands DoS attacks up to line speed
- Over 100,000 queries/sec
- Proven, RFC compliant DNS
- Interoperates with BIND, Windows
- Digitally signed code
  - TPM
- Redundant H/W capability
  - Dual power supplies
  - RAID
- Remote HP iLO2 management

SECURE64

Technical Conclusions

- Relying Only on Emerging H/W & S/W Technologies
  - Leaves Major Security Problems Unsolved
  - Does Not Produce a Genuinely Secure System
  - Loses Customer Benefits from:
    - Genuinely Secure S/W Structure
- Architecture for Genuinely Secure Systems
  - Exists today
  - Demonstrates the Needed S/W Structure
  - Shows Unmatched Security and Performance
  - Completes and Complements Major System Directions

SECURE64

Summary

- Important emerging H/W technologies
  - Stronger focus on system security
  - I/O Isolation and Access Protections
  - Generation, Retention of Root Secrets
- Important emerging S/W technologies
  - Traditional plus TPM (Unix, Linux, Vista©)
  - Virtualization
  - Architecture for Genuinely Secure Systems
- Unique Itanium® 2 architecture enables:
  - Genuinely Secure Systems and Secure Virtualization
- Genuinely Secure Systems will exist
  - One is shipping today

SECURE64